REMARKS

Claims 1-12 are pending in this application.

Rejection of Claims 1-6, 8 and 10-12 under 35 USC § 103(a)

Claims 1-6, 8 and 10-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linnartz (U.S. Patent No. 6,314,518) in view of Ranger et al. (U.S. 6,393,568). The Applicants respectfully request the Examiner to reconsider his rejection.

The present claimed invention, as defined by Claim 1, relates to a method for protection against the copying of digital data stored on a storage medium. The method includes identifying whether the digital data are encrypted and whether the digital data are watermarked. One of a permission and prohibition to copy and/or to play the digital data are delivered as a function of an identification of the encryption of the digital data and watermarking of the digital data.

Stated otherwise, in the method of our invention, a storage medium containing data is checked (examined) to determine whether the digital data that it contains can be played back (e.g. for video data, it is checked whether the video data can be displayed on a screen) or can be copied (i.e. duplicated in another storage medium) or in the contrary if the data cannot be played back or cannot be copied.

As admitted by the Office Action, Linnartz does not show or suggest encrypted digital data. Linnartz describes a method and system for transferring content information and supplemental information related thereto. The supplemental information includes a control pattern which is applied to a one-way function to generate a watermark. The control pattern and watermark form a cryptographically controlled counter. The counter is decreased in the player before the processed control pattern is provided to a recorder thereby allowing a limited number of generations of copies to be produced. As soon as the counter is decreased too often, the pattern will no longer match the watermark and reproduction will be blocked.

Should the watermark or control pattern be altered or manipulated, the quality of the reproduced content will be severely degraded.

Linnartz, as admitted in the Office Action, neither discloses nor suggests "identifying whether said digital data are encrypted" as recited in the present claimed invention. Linnartz also neither discloses nor suggests "identifying whether said digital data are watermarked" as recited in the present claimed invention. Linnartz adds a watermark by applying a one-way function to the control pattern. The watermark and control pattern form the supplemental information. There is no need in Linnartz to identify whether the digital data are watermarked as in the present claimed invention as the watermark is part of the supplemental information being recorded or reproduced. Linnartz is not concerned with identifying whether the digital data are watermarked, Linnartz is concerned with providing an integrity check by comparing the watermark with the processed control pattern to determine if they match. If the watermark does not match a valid control pattern, reproduction or recording may be controlled or blocked. As Linnartz neither discloses nor suggests identifying whether the digital data is encrypted and watermarked, Linnartz cannot disclose or suggest "delivering one of a permission and a prohibition to copy and/or to play said digital data as a function of an identification of: an encryption of said digital data; and a watermarking of said digital data" as in the present claimed invention.

Ranger et al. describes a computer based encryption and decryption system with a content analysis provision. This system is concerned with detecting computer viruses. The system generates a decryption request to decrypt the encrypted digital input information prior to applying content analysis such as virus detection. Ranger et al. was cited to illustrate determining if data is encrypted. Although Ranger et al. does detect whether digital input information is encrypted, upon detecting the digital input is encrypted, the information is decrypted for analysis. Ranger addresses the problem of detecting viruses in encrypted documents (see col. 1, lines 18-23) since it is noted in Ranger et al. that the detection of viruses is not reliable with encrypted documents. He therefore proposes to detect first whether a document is encrypted to decrypt it, if necessary, before applying the virus detection process (see col.2, lines 47-56 and Fig. 2, steps 30 and 32).

However, Ranger et al. is not concerned with "delivering one of a permission and a prohibition to copy and/or to play said digital data" as in the present claimed invention. Additionally, similarly to Linnartz, Ranger et al. neither disclose nor suggest "identifying whether said digital data are watermarked" as recited in the present claimed invention. Furthermore, Ranger et al., similarly to Linnartz, neither disclose nor suggest "delivering one of a permission and a prohibition to copy and/or to play said digital data as a function of an identification of: an encryption of said digital data; and a watermarking of said digital data" as in the present claimed invention.

The Examiner has asserted that it would have been obvious to one skilled in the art to combine the teachings of Linnartz with the teaching of Ranger et al. Ranger et al. and Linnartz are directed to entirely different and unrelated technologies. Linnartz is directed to protection against unauthorized reproduction and recording of data. Ranger attempts to detect viruses in encrypted documents. Ranger et al. teaches that in order to detect viruses, the encrypted document must first be decrypted. The decrypted data is then subject to a virus scan to detect viruses. The Applicants submit that there is no reason to combine the subject matter of Ranger et al. with the subject matter of Linnartz.

In the "Response to Arguments" section of the Office Action, it is stated at the end of the last paragraph (page 3):

> "*Ranger's teachings would help prevent Linnartz's system from being accidentally infected by a virus if the file was encrypted since Ranger's teachings would allow Linnartz to detect if the file was encrypted, thus requiring that the file be decrypted for virus scan.*"

Therefore, as correctly pointed out by the Office Action, the combination of the Linnartz system with the Ranger solution "*would prevent Linnartz's system from being infected with a virus*" (see page 4, lines 10-12 of the Office Action). However, this would not render obvious the subject matter of Claim 1. The Applicant agrees that "Linnartz does not prohibit use of encryption with his data" as stated by the Office Action. Applicants also agree that

Ranger discloses to "determine whether digital input information is encrypted" (col. 2, line 47-48) in order to decrypt the digital information to apply a virus detection mechanism. However, the only purpose of detecting whether the data are encrypted in Ranger is to decrypt them before applying this virus detection mechanism. This is very different from the present claimed invention which is concerned with copy protection and preventing unauthorized reproduction.

Therefore, Applicants submit that neither Linnartz nor Ranger et al. disclose identifying (i.e. to detect) whether data contained in a storage medium are encrypted **in combination** with the detection of a watermark in the data **to determine whether playback of the data or the copy of the data is permitted or prohibited** as claimed in claim 1 of the present invention.

Furthermore, even if Linnartz and Ranger et al. were combined, the combined system still would not make the present claimed invention unpatentable. The combination of Linnartz and Ranger et al. would produce a system that compares a system generated watermark with a control pattern to determine if data can be reproduced and if the data is encrypted, it is decrypted to detect for viruses. This combination still neither discloses nor suggests the present claimed invention. More specifically, neither Linnartz nor Ranger et al. when taken alone or in combination disclose or suggest "identifying whether said digital data are watermarked" or "delivering one of a permission and a prohibition to copy and/or to play said digital data as a function of an identification of: an encryption of said digital data; and a watermarking of said digital data" as in the present claimed invention.

Claim 2 is considered patentable based on its dependence on claim 1. Claim 2 is further considered patentable as Linnartz and Ranger et al. neither disclose nor suggest the features of claim 2. More specifically, as discussed above concerning claim 1, Linnartz and Ranger et al. neither disclose nor suggest "delivering a permission for digital copying when: ... - a watermarking of said digital data has been identified". Additionally, the Office Action cites Column 4, lines 1-45 of Linnartz as showing identifying the type of storage medium as claimed in claim 2. The cited passage of Linnartz actually discusses generating the

watermark from the control pattern and comparing the watermark to the control pattern. The cited passage and elsewhere of Linnartz is silent as to identifying the type of storage medium. Furthermore, the cited passages (column 4, lines 1-18 and Column 5, lines 25-44) of Linnartz neither disclose nor suggest "delivering a permission for digital copying when: ... - a non-recordable type of storage medium has been identified". The first cited passage identifies the Brief Description of the Drawings and the second cited passage discusses embedding a watermark in the data signal. The cited passage and elsewhere in Linnartz is silent regarding "delivering a permission for digital copying when: ... - a non-recordable type of storage medium has been identified" as claimed in claim 2.

Claims 3-6, 8, 10 and 11 each include features which further define claim 1 and are similar to features of claim 2. These claims are dependent on claim 1 and are thus considered patentable for the same reasons as claim 1. The arguments provided regarding claim 1 and 2 are also applicable to the features of claims 3-6, 8, 10 and 11.

Claims 8 and 12 are dependent indirectly on claim 1 and thus are considered patentable for the reasons discussed above regarding claim 1.

In view of the above remarks it is respectfully submitted that there is no 35 USC 112 compliant enabling disclosure in Linnartz and Ranger et al., when taken alone or in combination, showing the above discussed features. It is thus, further respectfully submitted that this rejection is satisfied and should be withdrawn.

Rejection of Claim 7 under 35 USC § 103(a)

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Linnartz (U.S. Patent No. 6,314,518 B1) in view of Ranger et al. (U.S. Patent No. 6,393,968) and further in view of Ichinoi (U.S. Patent No. 6,266,477).

Ichinoi describes a data signal recording and playback method and system for determining whether the recording medium being used is a high or standard performance

medium and selecting recording specifications accordingly. Ichinoi was cited to show conversion of digital data into analog signals and corrupting the analog signals if a prohibition of digital copying is delivered. However, Ichinoi, similarly to Linnartz and Ranger et al., neither discloses nor suggests "identifying whether said digital data are watermarked" or "delivering one of a permission and a prohibition to copy and/or to play said digital data as a function of an identification of: an encryption of said digital data; and a watermarking of said digital data" as claimed in claim 1 of the present claimed invention.

In view of the above remarks and amendments to the claims it is respectfully submitted that there is no 35 USC 112 compliant enabling disclosure in Linnartz, Ranger et al. and Ichinoi, when taken alone or in combination, showing the above discussed features. It is thus, further respectfully submitted that this rejection is satisfied and should be withdrawn.

Rejection of Claim 9 under 35 USC § 103(a)

Claim 9 is rejected under 35 U.S.C. 103 (a) as bring unpatentable over Linnartz (U.S. Patent No. 6,314,518) in view of Ichinoi (U.S. Patent No. 6,266,477) and further in view of Ranger et al. (U.S. Patent No. 6,393,568).

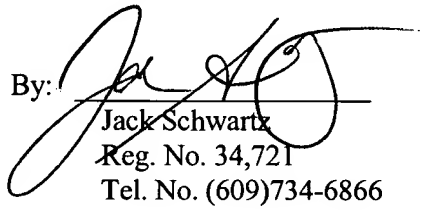
Claim 9 provides a device for playing digital data stored on a storage medium, including means for detecting whether the digital data are encrypted, and a copy protection system being able to receive signals from the means for detecting to generate a copy permission signal or a copy prohibition signal, as a function of the signals received from the means for detecting. Claim 9 is a device claim including features similar to those discussed above regarding claim 1 as well as additional features similar to those claimed in claims 2-8 and 10-12. Thus, as discussed above regarding the rejections of claim 1 and 7, none of Linnartz, Ranger et al. and Ichinoi, when taken alone or in combination, disclose or suggest "identifying whether said digital data are watermarked" or "delivering one of a permission and a prohibition to copy and/or to play said digital data as a function of an identification of: an encryption of said digital data; and a watermarking of said digital data" as claimed in claim 1 of the present claimed invention.

In view of the above remarks and amendments to the claims it is respectfully submitted that there is no 35 USC 112 compliant enabling disclosure in Linnartz, Ranger et al. and Ichinoi, when taken alone or in combination, showing the above discussed features. It is thus, further respectfully submitted that this rejection is satisfied and should be withdrawn.

Having fully addressed the Examiner's rejections, it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at the phone number below, so that a mutually convenient date and time for a telephonic interview may be scheduled.

No additional fee is believed due. However, if an additional fee is due, please charge the additional fee to Deposit Account 07-0832.

Respectfully submitted,
Sylvain Chevreau et al.

By: 
Jack Schwartz
Reg. No. 34,721
Tel. No. (609)734-6866

Thomson Licensing, LLC
Patent Operations
PO Box 5312
Princeton, NJ 08543-5312
September 19, 2007

CERTIFICATE OF MAILING under 37 C.F.R. §1.8

I hereby certify that this amendment is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

Date: September 19, 2007

Jack Schwartz
Reg. No. 34,721